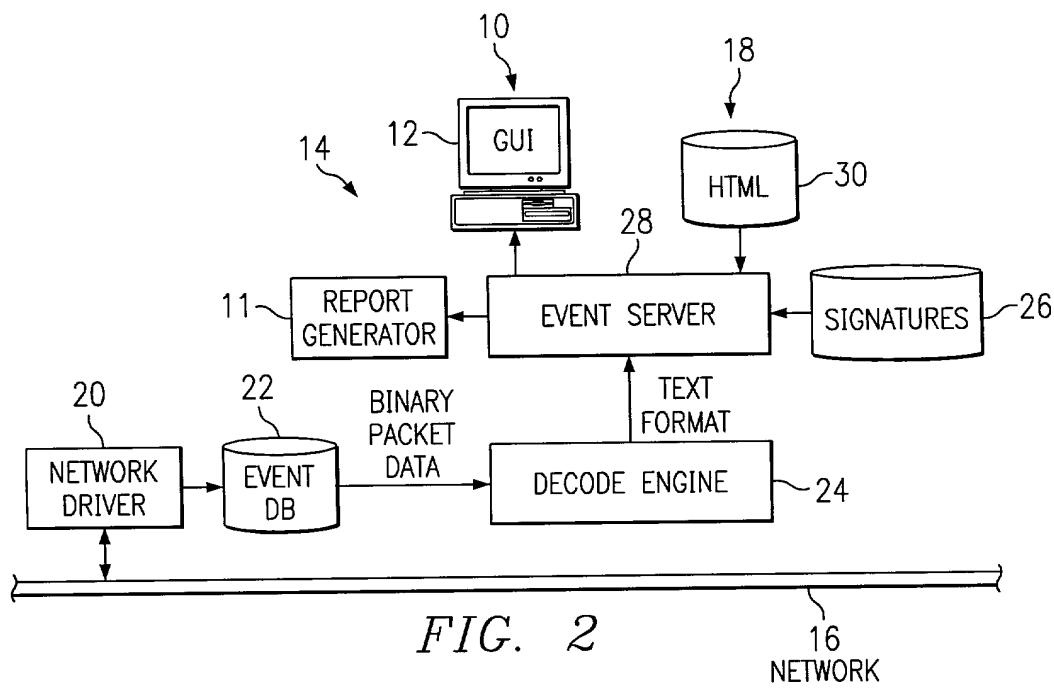10017330-1
Richard L. Schertz, et al.
User Interface for Presenting Data
for an Intrusion Protection System
1/4

FIG. 1

FIG. 2

10017330-1
Richard L. Schertz, et al.
User Interface for Presenting Data
for an Intrusion Protection System
2/4

40 — (INTRUSION GUI)

42 — GENERATE SIGNATURE TO DECODED DATA MAPPING

44 — DISPLAY EVENT SIGNATURE

46 — DISPLAY DECODED EVENT DATA

48 — EVENT SIGNATURE COMPONENT SELECTED? —NO

↓YES

50 — HIGHLIGHT CORRESPONDING DECODED EVENT DATA

DECODED EVENT DATA SELECTED? —NO

52

↓YES

54 — HIGHLIGHT CORRESPONDING EVENT SIGNATURE COMPONENT
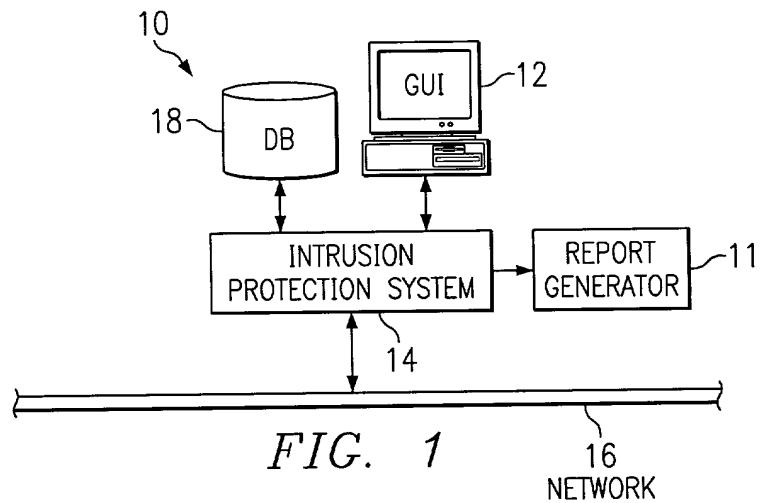
EXIT? —NO

56

↓YES

58 — (END)

FIG. 3

10017330-1
Richard L. Schertz, et al.
User Interface for Presenting Data
for an Intrusion Protection System
3/4

70 — (INTRUSION GUI)

72 — | GENERATE SIGNATURE TO DECODED DATA MAPPING TABLE |

74 — | DISPLAY ETHERNET HEADER DATA SUMMARY |

76 — | DISPLAY IP HEADER DATA SUMMARY |

78 — | DISPLAY IP HEADER DATA |

FIG. 4

80 — | DISPLAY EVENT SIGNATURE |

82 — < EVENT SIGNATURE COMPONENT SELECTED? > — NO

YES

84 — | HIGHLIGHT CORRESPONDING IP HEADER DATA AND SUMMARY |

< IP HEADER DATA SELECTED? > — NO

86 YES

88 — | HIGHLIGHT CORRESPONDING IP HEADER DATA SUMMARY AND SIGNATURE |

< IP HEADER DATA SUMMARY SELECTED? > — NO

90 YES

92 — | HIGHLIGHT CORRESPONDING IP HEADER DATA AND SIGNATURE |

< EXIT? > — NO

YES 94

END — 96

10017330-1
Richard L. Schertz, et al.
User Interface for Presenting Data
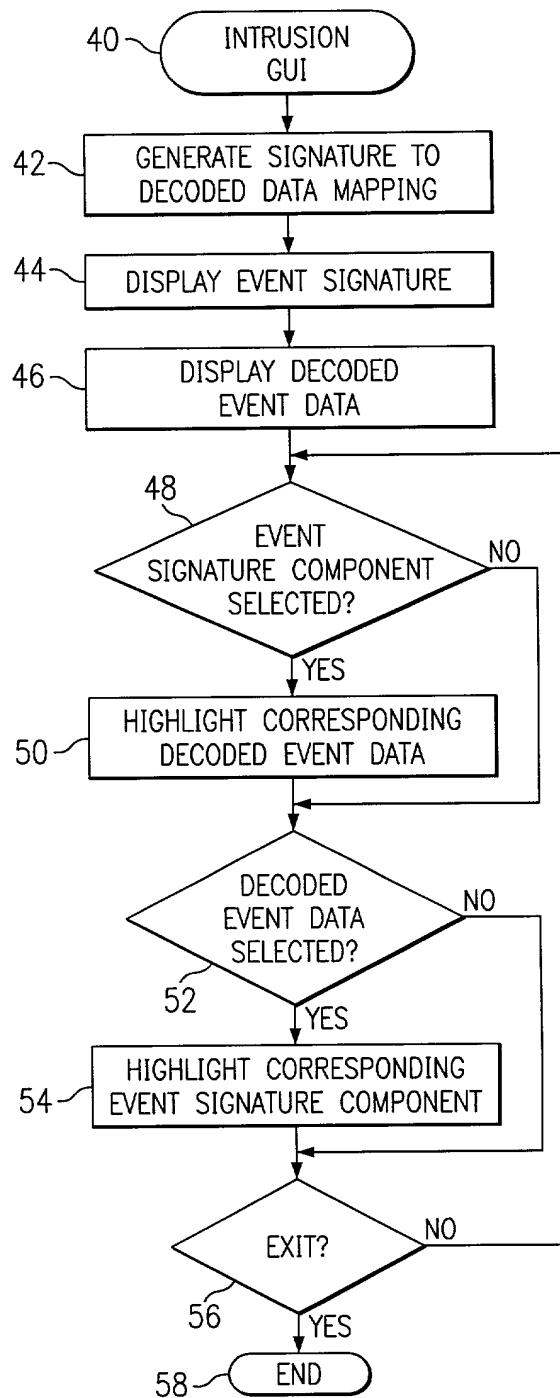for an Intrusion Protection System
4/4

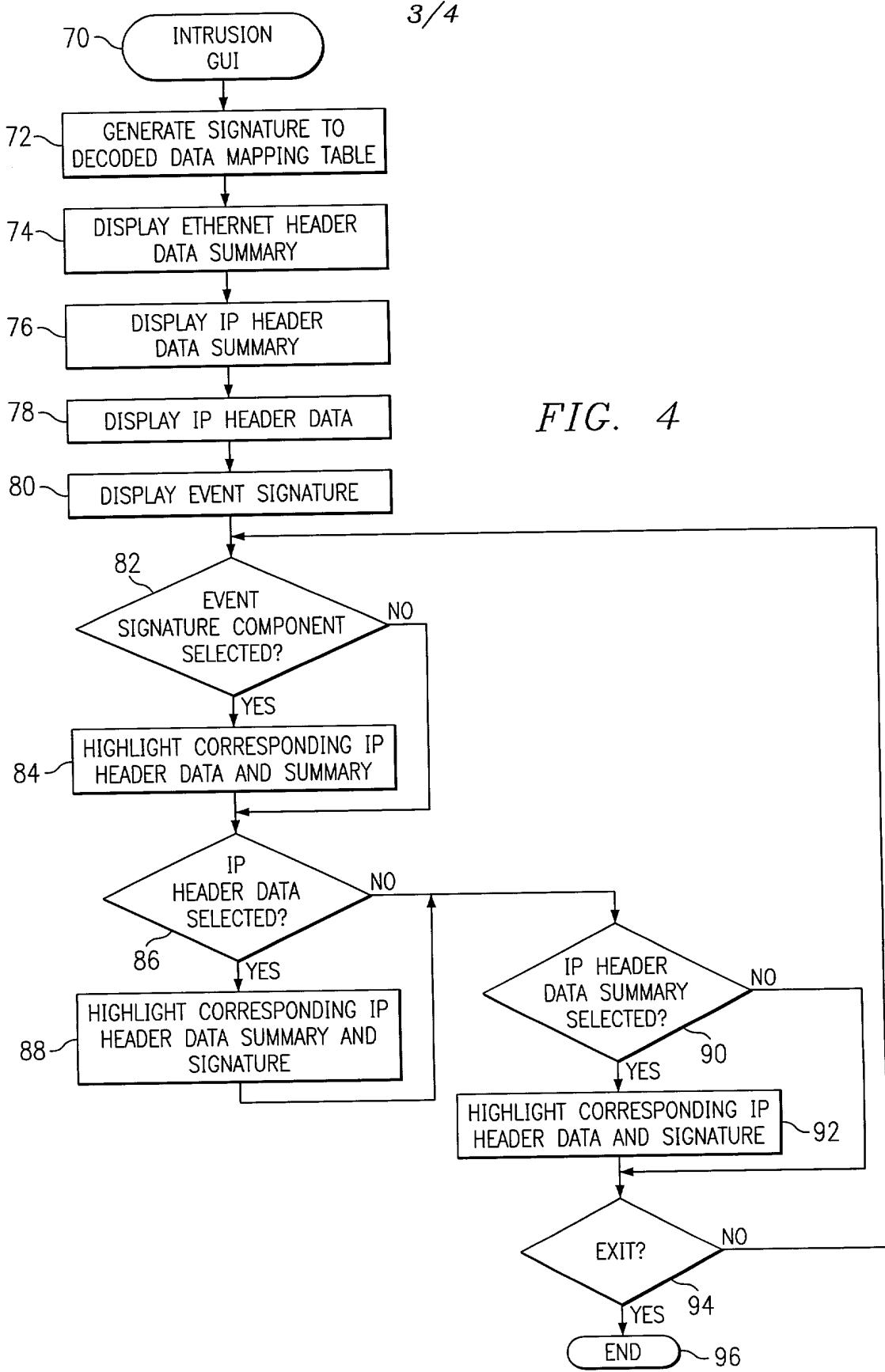*FIG. 5*   100

HP Netaction Attack Defender   ▭ 回 ✕

File View Help

HP Attack Defender   122 → (Start) (Stop) (Reset)

System	(Back) Detailed Results

(Back) **Detailed Results**
Ping of Death: 1 of 1 Prevented

System
Intrusions
Attacks
Recon
SvcMgmt
Policy
Reports
Log

↑
120

Signature: (icmp) & (65535 < ((ip[2:2] – ((ip[0:1] 0x0f) * 4))
+ ((ip[6:2]_0x1fff) * 8))))   ⟋102
                                    110

————————— ETHER Header —————————
ETHER: Destination: Accton-9A-0C-61 (00-00-E8-9A-0C-61)
ETHER: Source: 00-C0-4F-14-9D-81
ETHER: Protocol: IP   ⟋104

————————— IP Header —————————
IP: Version = 4
IP: Header length = 20
IP: Differentiated Services (DS) Field = 0x00   106
IP: 0000 00.. DS Codepoint = Default PHB (0)   ⟋
IP: .... ..00 Unused
IP: Packet length = 1500 (1372 bytes missing) ⟍112
IP: Id = 10e1
IP: Fragmentation Info = 0x1FCC
IP: .0.. .... Don't Fragment Bit = FALSE
IP: ..0. .... More Fragments Bit = FALSE
IP: ...1 1111 1100 1100 Fragment offset = 65120
IP: Time to live = 255
IP: Protocol = ICMP (1)
IP: Header checksum = 7066
IP: Source address = 10.1.1.2
IP: Destination address = 10.0.0.11
IP: Continuation of a missing packet   108
       114   ⟋

0000: 00 00 E8 9A 0C 61 00 C0 – 4F 14 9D 81 08 00 45 00   ....
0010: 05 DC 10 E1 1F CC FF 01 – 70 66 0A 01 01 02 0A 00   ....
0020: 00 0B 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00   ....
0030: 00 00 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00   ....
0040: 00 00 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00   ....
0050: 00 00 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00   ....
0060: 00 00 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00   ....
0070: 00 00 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00   ....
0080: 00 00 00 00 00 00 00 00 – 00 00 00 00 00 00   ....

◀